VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

E-Voting Through Homomorphic Encryption

Project-Report

CSE3502 - Information Security Management

Under the guidance of

Dr Selvi. M

Submitted by:

Utkarsh Tikkiwal (20BCE0334)

Rishabh Agrawal (20BCE0798)

Zaman Saleel (20BCE2025)

ABSTRACT:

This project aims to develop an e-voting system using Paillier's homomorphic encryption algorithm, which provides a high level of security and privacy in the voting process. The proposed system allows voters to cast their ballots from any location using their personal devices, such as smartphones or computers, and ensures the integrity of the voting process by encrypting and decrypting votes while maintaining their anonymity. The system utilizes a decentralized approach to the vote counting process, making it less vulnerable to attacks and manipulation. The system is implemented in C++. The project will be evaluated based on its efficiency, security, and usability, and will contribute to the ongoing efforts to modernize the electoral process and promote democracy worldwide.

INTRODUCTION:

Background

A manual voting process is one where the votes are recorded manually. Such a system is extremely time consuming when it actually has to be carried out. Before declaring the results, a huge amount of time is needed to tally the number of votes. It is also quite difficult for physically challenged people to cast their vote through such a system, requiring them to nominate someone to cast the vote on their behalf.

Casting votes using paper ballots, as is the case in most manual voting processes, is also quite risky in addition to being time-consuming. There is a high chance of the system being cheated through the submission of bogus paper votes in the ballot. It is a challenging task to identify the honest votes and maintain security and integrity in the voting process with the use of such systems.

Motivation

The development of our e-voting system is driven by the need to enhance the efficiency, accessibility, and security of the voting process. Traditional voting methods have long been associated with challenges such as long queues, low voter turnout, and instances of fraud and tampering. An e-voting system can help to address these issues by enabling voters to cast their ballots from anywhere in the world, reducing the likelihood of human error and ensuring that every vote is accurately counted. Furthermore, the implementation of the homomorphic encryption ensures that the privacy of each voter is strictly maintained and tampering cannot be performed since the outcome is only known after decrypting the final results.

Additionally, an e-voting system can provide increased transparency and security measures, allowing voters to have confidence in the integrity of the electoral process. Overall, the development of an e-voting system can help to increase voter participation, improve the accuracy of election results, and strengthen the democratic process.

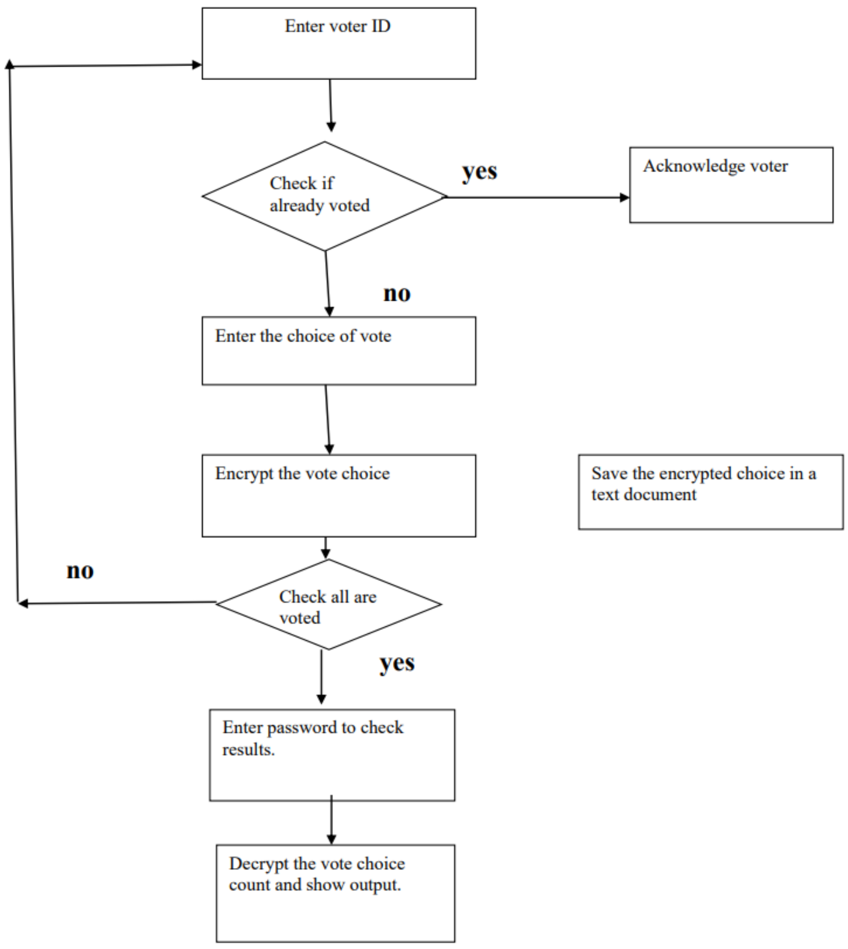
Aim of the proposed Work

The votes polled by voters are encrypted and using a homomorphic encryption technique without idea of plain data directly computation is performed on encrypted data and results are declared with plain output data by decryption. So, voting privacy is protected and its an efficient way to eradicate many problems with general voting. We can even reach remote locations with e- voting. People can cast their vote from any place on the globe over the internet. People can open the authorised website and can easily cast their vote to their candidate at anyplace and anytime they want.

PROPOSED METHODOLOGY:

We proposed an E-Voting mechanism using the Paillier Homomorphic Encryption technique which can be used to provide security to the voting system and to help us manipulate and transfer data in encrypted form to other authorised places making it impenetrable by others. We use the Paillier Encryption's homomorphic property that allows us to add the votes in encrypted form and when decrypted will give us the original number of votes polled after computation on cipher data.

Paillier's cryptosystem has additive homomorphism which makes it an excellent choice to add the results of an election. In Paillier's homomorphic addition, the product of two cipher data will decrypt to the sum of their corresponding plain data.



LITERATURE REVIEW:

PAPER – 1

TITLE: Blinded additively homomorphic encryption schemes for self-tallying voting

AUTHOR: Lafitte, Dossogne

YEAR: 2015

PUBLISHER: Elsevier Ltd

SUMMARY:

This paper discusses the self-tallying election protocol based public key homomorphic encryption. The additive homomorphism allows a set of participants (voters) to publish an encrypted value (ballot) and to compute the encrypted sum of all these values based on their ciphertexts. This scheme has the particularity that anyone can decrypt the sum, but only once all participants have contributed to its computation. More precisely, the sum can be decrypted at all times, but remains blinded until all participants have contributed their vote, which contains a share of the unblinding key.

ADVANTAGES:

The use of blinded encryption ensures that no one, including the voting authorities, can link a specific vote to a specific voter. This provides strong privacy guarantees for voters, which can help to increase voter confidence in the voting system.

LIMITATIONS:

The article includes the assumption of an honest majority of voters, lack of coercion resistance, limited support for complex operations, and the need for further evaluation in real-world scenarios.

PAPER – 2

TITLE: Homomorphic encryption method applied to Cloud Computing

AUTHOR: Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI

YEAR: 2012

PUBLISHER: IEEE

SUMMARY:

This paper proposes the use of homomorphic encryption in cloud computing to perform computations on encrypted data without decryption, thereby ensuring privacy and security of sensitive information stored in the cloud. The paper discusses the challenges faced by cloud computing providers in ensuring data security and proposes the use of homomorphic encryption to overcome these challenges. The paper provides a detailed explanation of homomorphic encryption, its existing systems, and its limitations. The paper also presents a proposed system that uses proxy re-encryption technique to prevent ciphertext from chosen ciphertext attacks.

ADVANTAGES:

The paper proposes a solution to the critical problem of ensuring privacy and security of sensitive information stored in the cloud. The proposed system provides a way to perform computations on encrypted data without decryption, ensuring privacy and security of the data. The paper also provides a detailed explanation of homomorphic encryption, its existing systems, and its limitations.

LIMITATIONS:

The paper does not provide a detailed analysis of the performance of the proposed system, which is an important consideration when implementing a practical solution. The paper also does not discuss the potential impact of homomorphic encryption on the performance of cloud computing systems. Additionally, the paper does not provide a detailed analysis of the potential security risks associated with homomorphic encryption, which is an important consideration when implementing a secure system.

PAPER – 3

TITLE: Filling the gap between voters and cryptography in e-voting

AUTHOR: Han, Chen, Zheng

YEAR: 2009

PUBLISHER: Elsevier Ltd

SUMMARY:

A new voting system is presented in this paper to combine the advantages of the voting scheme of MoranNaor and the voting scheme based on homomorphic encryption. The voter is free of complicated computation and more advantages are given: the ballots can be recovered when the voting machine breaks down, the costly cut-and-choose zero-knowledge proofs made by the voting machine are avoided and the partial tally result in each voting machine is kept secret.

ADVANTAGES:

It focuses on involving voters in the design of e-voting systems. The authors recognize that the best way to improve the usability and security of e-voting systems is to involve the people who will be using them. By engaging with voters and soliciting their feedback, e-voting systems can be designed to better meet the needs and expectations of voters.

LIMITATIONS:

The proposed solutions to bridge the gap between voters and cryptography may not be sufficient to address all of the usability and security challenges of e-voting systems. It does not address some of the more technical challenges of e-voting systems

PAPER – 4

TITLE: Privacy preserving E-voting cloud system based on ID based encryption

AUTHOR: Shankar, Stephan, Pandiaraja, Sumathi, Sharma

YEAR: 2021

PUBLISHER: Springer

SUMMARY:

In this paper, a model to poll a vote in a secure way that can avoid false voting based on their user functions in the online e-voting system is developed. In the proposed system, the cubic structure for storing the voting details is provided which is based on the CCK. To search and verify the data, the data is decrypted and sent to the user from the cloud. Then security and performance analysis is discussed which clearly shows that the proposed method is efficient for online e-voting systems when compared with the existing schemes

ADVANTAGES:

It uses ID-based encryption, which simplifies key management and eliminates the need for a public key infrastructure which reduces the complexity of the system and makes it easier to implement and maintain. It also uses cloud computing, which enables the system to be scalable and efficient. The system can handle a large number of voters and perform computations quickly, which is important for a successful e-voting system.

LIMITATIONS:

The proposed system has a reliance on a single cloud provider. While the use of cloud computing enables scalability and efficiency, it also introduces a single point of failure. If the cloud provider experiences an outage or security breach, the entire system could be compromised.

PAPER – 5

TITLE: Advanced e-voting system using Paillier homomorphic encryption algorithm

AUTHOR: Anggriane, Nasution, Azmi

YEAR: 2017

PUBLISHER: IEEE

SUMMARY:

This paper proves the effectiveness of the Paillier algorithm and its homomorphic property that is implemented in an e-voting system. With homomorphic property, the system can calculate the sum of votes in ciphertext form without revealing the choice of the voters. The resulting ciphertext values will be different each other even though the same plaintext is encrypted, with a size of 4 times larger than the plaintext size

ADVANTAGES:

The system guarantees data confidentiality and utilises homomorphic properties of the algorithm to calculate the votes that are processed by the system. The success ratio of the system to perform calculation is 100%. Systems with Paillier homomorphic algorithms can accommodate input plaintext up to the values of n. The resulting ciphertext value is different from each other though the plaintext to be encrypted has the same value.

LIMITATIONS:

Limitation of the proposed system is the reliance on a trusted authority to generate the public and private keys used in the Paillier encryption scheme. This could potentially introduce a single point of failure if the trusted authority is compromised. Another problem is the complexity of the system, which could make it difficult for some users to understand and use. This could potentially discourage some voters from using the system or increase the risk of user errors.

PAPER – 6

TITLE: Cryptographic vote-stealing attacks against a partially homomorphic e-voting architecture

AUTHOR: Tsoutsos N.G., Maniatakos M.

YEAR: 2016

PUBLISHER: IEEE

SUMMARY:

This paper discusses the security of a partially homomorphic electronic voting architecture and presents a vote-stealing attack by exploiting a length-extension vulnerability in the message authentication component of the system. The paper analyses the security of the election infrastructure and presents a cryptographic vote-stealing attack that exploits a length-extension vulnerability on the underlying message authentication scheme. The attack leverages the homomorphic properties of the Paillier cryptosystem and by forging negative vote balances for the actual winning party, enables a malicious party to modify the reported election results.

ADVANTAGES:

The paper sheds light on the vulnerabilities of an electronic voting architecture and highlights the importance of secure e-voting protocols. It presents a concrete attack that can be used to modify election results and provides details of how the attack can be carried out. The paper also discusses potential mitigations to the vulnerability and provides recommendations for improving the security of electronic voting systems.

LIMITATIONS:

The paper discusses the vulnerabilities of a specific electronic voting architecture, and the attack presented may not be applicable to other systems. The paper also assumes that the attacker has access to the underlying code of the system, which may not be possible in all cases. Additionally, the paper focuses on the Paillier cryptosystem and does not provide an analysis of other encryption schemes that may be used in electronic voting systems. The paper does not provide a detailed evaluation of the security of other components of the electronic voting architecture, such as the authentication system.

PAPER – 7

TITLE: Use case of Paillier Homomorphic Algorithm for Electronic-Voting Systems

AUTHOR: Roopa K, Gokul B.S., Arakalgud S.K

YEAR: 2021

PUBLISHER: IEEE

SUMMARY:

The paper discusses the need for cryptographic algorithms with homomorphic properties to protect confidential data during processing without compromising its security. Paillier cryptosystem is presented as an example of such an algorithm. The paper focuses on the use case of an e-voting system, which is implemented using the Paillier cryptosystem and analysed using Python programming language. The paper proposes a new voting scheme based on two stages of encryption and a digital envelope for critical security requirements.

ADVANTAGES:

The paper discusses the need for cryptographic algorithms with homomorphic properties to protect confidential data during processing without compromising its security. Paillier cryptosystem is presented as an example of such an algorithm. The paper focuses on the use case of an e-voting system, which is implemented using the Paillier cryptosystem and analysed using Python programming language. The paper proposes a new voting scheme based on two stages of encryption and a digital envelope for critical security requirements.

LIMITATIONS:

The paper does not discuss the potential drawbacks or limitations of using the proposed solution. The paper also does not address the practicality or feasibility of implementing the proposed e-voting system in a real-world scenario. Additionally, the paper does not provide any comparison or evaluation of the proposed solution with other existing solutions.

PAPER – 8

TITLE: Filling the gap between voters and cryptography in e-voting

AUTHOR: Han W, Chen K.F., Zheng D.

YEAR: 2009

PUBLISHER: Elsevier

SUMMARY:

The paper proposes a new e-voting system that combines the advantages of Moran-Naor's voting scheme and voting scheme based on homomorphic encryption to make use of cryptography while hiding the details of cryptographic computation from voters. The proposed system solves the problem of ballot restoration in Moran-Naor's scheme, improves efficiency, and simplifies the design of the directed recording electronic (DRE) voting machine.

ADVANTAGES:

The proposed e-voting system combines the advantages of Moran-Naor's voting scheme and homomorphic encryption-based voting schemes, providing verifiability while hiding the complexity of cryptographic computation from voters. The system allows for the recovery of ballots if the voting machine breaks down and avoids the costly cut-and-choose zero-knowledge proofs for shuffling votes made by the voting machine. The partial tally result in each voting machine can be kept secret, ensuring fairness and privacy.

LIMITATIONS:

The proposed system assumes a 1-out-of-L election, which may not be suitable for all types of elections. The paper does not provide a detailed analysis of the system's security, and the proposed system may require further testing and validation before implementation in real-world scenarios.

PAPER – 9

TITLE: Enhanced E-voting protocol based on public key cryptography

AUTHOR: Almimi H.M., Shahin S.A, Al Fayoumi M, Daoud M.S., Ghadi Y.

YEAR: 2019

PUBLISHER: IEEE

SUMMARY:

The paper proposes an e-voting protocol that uses public key encryption and two pairs of certificates, one for citizens and one for the National Information Technology Center (NITC) acting as a trusted certificate authority. The protocol addresses security requirements such as confidentiality, integrity, authentication, non-repudiation, and audibility. The paper also discusses technical, political, cultural, and legal obstacles to e-voting.

ADVANTAGES:

The proposed model relies on public key encryption, which is a well-established and widely-used method for securing electronic communications. This could make the proposed e-voting system more robust and resistant to attacks. The proposed e-voting system is designed to be auditable and verifiable, which could help increase public trust in the electoral process. This could ultimately lead to higher voter turnout and increased participation in the democratic process.

LIMITATIONS:

The paper does not address all obstacles to e-voting, such as the potential for technical malfunctions or hacking. The paper also assumes that the NITC is an objective and neutral party, which may not always be the case in practice. Additionally, the paper acknowledges potential security issues with using a web interface for key exchange and typing in a key, but does not provide solutions to these issues.

PAPER – 10

TITLE: A secure verifiable ranked choice online voting system based on homomorphic encryption

AUTHOR: Yang X, Yi X., Kelarev A., Han F., Nepal S.

YEAR: 2018

PUBLISHER: Elsevier

SUMMARY:

The paper proposes a ranked choice online voting system that uses the exponential ElGamal cryptosystem to encrypt ballots before submission to protect confidentiality. The system generates cryptographic proofs to ensure the integrity and validity of each vote before counting. The proposed system eliminates hardwired restrictions on the possible assignments of points to different candidates based on voters' personal preferences. The security and performance analyses show that the proposed method achieves significant improvements compared to previous systems.

ADVANTAGES:

The proposed system allows voters to assign points to candidates based on their personal preferences without restrictions. The system ensures the confidentiality of votes by encrypting each cast ballot before submission. The cryptographic proofs generated by the system verify the validity and eligibility of each vote before counting without decrypting the content of the ballot. The proposed system achieves significant improvements in security and performance compared to previous systems. The system reduces the overall cost of running elections and promotes sustainability.

LIMITATIONS:

The proposed system requires advanced security methods that may be challenging to implement in practice. The system relies on the exponential ElGamal cryptosystem, which may have limitations in terms of scalability and efficiency. The proposed system may require additional resources for voter education and training to ensure proper usage and understanding of the system. The system may be vulnerable to hacking attacks, and continuous updates and improvements may be necessary to address emerging security threats.

PAPER – 11

TITLE: Group homomorphic encryption: characterizations, impossibility results, and applications.

AUTHOR: Armknecht, Frederik,Katzenbeisser, Stefan,Peter, Andreas

YEAR: 2012

PUBLISHER: Springer

SUMMARY:

The paper proposes an abstract and unified formulation of a class of homomorphic encryption schemes called group homomorphic encryption schemes of shift type. The authors characterise two standard security properties and show that their framework covers many existing homomorphic encryption schemes. They also discuss concrete constructions of homomorphic encryption schemes based on existing computational assumptions.

ADVANTAGES:

The paper provides a unified framework for homomorphic encryption schemes of shift type, which covers many famous schemes. The authors characterise the security properties of these schemes and provide concrete constructions based on existing computational assumptions. The paper's results have practical importance for various applications, such as e-voting and privacy-preserving data mining.

LIMITATIONS:

The proposed framework does not cover all homomorphic encryption schemes that are practically reasonable, such as those for which the encryption and homomorphic operations may generate invalid ciphertexts with negligibly small but non-zero probabilities. Additionally, the paper assumes the existence of certain computational assumptions and does not provide a proof of their security in the real world

PAPER – 12

TITLE: E-Voting System Using Blockchain and Homomorphic Encryption

AUTHOR: Naidu. P.R., Bolla. D.R., Prateek. G., Harshini. S.S., Hegde. S.A., Harsha. V.V.S.

YEAR: 2022

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

The paper discusses the need for secure and fair elections, given that only about half of the elections are deemed to be free and fair. The authors propose using homomorphic encryption and blockchain technology to ensure that only eligible citizens can vote, and to store voter data and vote cast in a local blockchain. The authors argue that this approach can provide a more secure and transparent way of conducting elections, while also providing unique insights into the election results.

ADVANTAGES:

The proposed system has several advantages. First, it ensures that only eligible citizens can vote, thereby preventing voter fraud. Second, it uses homomorphic encryption to secure voter data, which allows for statistical analysis while preserving privacy. Third, it uses blockchain technology to ensure the integrity and immutability of the election results. Fourth, it provides a more convenient and efficient way of conducting elections, as voters can cast their votes from any location with an internet connection.

LIMITATIONS:

The paper does not discuss the potential challenges and limitations of implementing the proposed system. For example, there may be technical challenges in developing and deploying a secure and reliable e-voting system that is accessible to all eligible voters. Additionally, there may be concerns about the security and privacy of voter data stored on a local blockchain, particularly if the blockchain is not properly secured. Finally, there may be legal and regulatory challenges in implementing such a system, as it may require changes to existing laws and regulations related to voting.

PAPER – 13

TITLE: Private computation of the Schulze voting method over the cloud.

AUTHOR: Yadav Vijay Kumar, Anand Anshul Verma, Shekhar Venkatesan S.

YEAR: 2020

PUBLISHER: Springer

SUMMARY:

The paper proposes an algorithm that uses fully homomorphic encryption (FHE) to compute the Schulze voting method privately, without revealing the preferences of the voter. The Schulze method involves computing the strength of the strongest path in a weighted graph, which is challenging to implement privately. The authors use the Levelled-Brakerski–Gentry–Vaikuntanathan (BGV) FHE scheme to compute the strongest paths using a modified version of the Floyd-Warshall algorithm. They evaluate their proposed algorithm using the HElib FHE library and investigate the impact of various parameters on computation time, communication complexity, and key size.

ADVANTAGES:

The proposed algorithm provides a way to compute the Schulze voting method privately, which can protect the sensitive information of voters. The use of FHE allows computation on encrypted data, ensuring that the output remains encrypted and private. The authors provide an evaluation of their algorithm, which can guide the selection of optimal parameters for efficient computation.

LIMITATIONS:

The proposed algorithm uses FHE, which is known to be computationally expensive and requires significant computational resources. The evaluation results show that increasing the number of levels in the modulus chain leads to increased computation and communication complexity. Therefore, the proposed algorithm may not be practical for large-scale applications, and there is a need for more efficient FHE schemes. The paper also assumes that the encryption scheme is secure and does not provide a formal proof of security.

PAPER – 14

TITLE: Okamoto-Uchiyama homomorphic encryption algorithm implementation in e-voting system

AUTHOR: Suwandi R., Nasution S.M., Azmi F.

YEAR: 2017

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

The article discusses the problems in electronic voting systems, including security, data confidentiality, and accuracy. It proposes using cryptography, specifically the Okamoto-Uchiyama algorithm, to encrypt the voting data and ensure its security and confidentiality. The algorithm also has homomorphic properties that allow mathematical calculations to be performed on encrypted data without decryption.

ADVANTAGES:

The use of cryptography can provide security, completeness, and authenticity of the voting data. The Okamoto-Uchiyama algorithm's homomorphic properties allow for secure and accurate vote counting without the need to decrypt the data, maintaining its confidentiality.

LIMITATIONS:

The article does not discuss potential challenges or limitations in implementing the Okamoto-Uchiyama algorithm in an electronic voting system. Additionally, the article does not provide empirical evidence or evaluation of the effectiveness of this algorithm in practice.

PAPER – 15

TITLE: An electronic voting system based on homomorphic encryption and prime numbers

AUTHOR: Azougaghe A., Hedabou M., Belkasmi M.

YEAR: 2016

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

The paper presents an electronic voting system based on homomorphic encryption to ensure privacy and confidentiality in voting. The proposed scheme uses multiplicative homomorphic encryption and separates privileges among voting participants to ensure privacy, anonymity, and reliability. The paper provides a review of related works, voting properties, and a system model. It also includes a detailed design and an example to evaluate the proposed scheme.

ADVANTAGES:

The proposed electronic voting system ensures privacy, confidentiality, and reliability. The use of multiplicative homomorphic encryption allows for mathematical calculations to be performed on encrypted data without the need for decryption, which adds an extra layer of security. The scheme separates privileges among voting participants, reducing the risk of a single point of failure.

LIMITATIONS:

The paper does not discuss the potential limitations or challenges in implementing the proposed system. The paper does not provide details on the scalability of the proposed scheme for large-scale elections. The paper assumes a cloud computing environment, which may not be applicable in all settings.

PAPER – 16

TITLE: Survey on Homomorphic Encryption

AUTHOR: Bansal V.

YEAR: 2021

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

This paper provides an introduction to homomorphic encryption, a technique used to perform computations on encrypted data without revealing the plaintext. The paper aims to present a literature survey on different homomorphic encryption techniques and classifications, as well as its applications in cloud computing, electronic voting, internet of things, and privacy preservation. The need for such techniques arises due to the high risk of data exposure on the internet, where users share critical personal information.

ADVANTAGES:

The paper discusses the advantages of homomorphic encryption, including its ability to preserve the structure or form of the data and its quantum-safe nature. The advantages of homomorphic encryption include secure data transmission, privacy preservation, and the ability to perform computations on encrypted data.

LIMITATIONS:

The limitations of homomorphic encryption include slower processing speed, higher computational requirements, and the need for a trusted entity to perform decryption.

PAPER – 17

TITLE: Secure voting in the cloud using homomorphic encryption and mobile agents

AUTHOR: Will M.A., Nicholson B., Tiehuis M., Ko R.K.L.

YEAR: 2016

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

The paper proposes a practical application of partially homomorphic encryption for a cloud-based mobile electronic voting scheme to address the challenges of declining voter turnout and the need for secure electronic voting. The paper introduces a new technique for users to verify their vote without a public bulletin board and evaluates the performance of the scheme on mobile devices and in the cloud. The paper also proposes the use of a dedicated hardware server for homomorphic tallying and decryption to improve system security.

ADVANTAGES:

The proposed electronic voting scheme offers the potential to increase voter turnout and simplify the voting process. The use of homomorphic encryption and a dedicated hardware server can address security concerns, and the new technique for verifying votes protects voter privacy.

LIMITATIONS:

The paper acknowledges that developing an e-voting scheme that is 100% secure against all attack vectors is difficult. The proposed scheme still faces security, privacy, and accountability concerns, and the use of mobile devices introduces new vulnerabilities. The proposed scheme has not been implemented or tested in a real-world setting, and the evaluation of the scheme's performance is limited to a benchmarking analysis.

PAPER – 18

TITLE: An anonymous voting system based on homomorphic encryption

AUTHOR: Zhao Y., Pan Y., Wang S., Zhang J.

YEAR: 2014

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

The paper presents an electronic voting system based on homomorphic encryption to ensure anonymity, privacy, and reliability in the voting. The system is designed to support the separation of privileges among voters, tellers, and announcers. The authors have divided the voting participants into three parties: voters, tellers, and announcers. Voters cast their ballots individually with no involvement in counting votes and announcing the results. Tellers are in charge of counting votes, and announcers are the designated publishers of the voting results.

ADVANTAGES:

The system ensures anonymity, privacy, and reliability in the voting process. The system supports the separation of privileges among voters, tellers, and announcers, which makes it more scalable, flexible, and convenient to use than the monolithic voting system. The use of homomorphic encryption provides a wide range of applications, including secure multi-party computation, database encryption, electronic voting, etc.

LIMITATIONS:

The paper does not discuss the implementation challenges and limitations of the system. The experimental results are not extensively discussed. The paper does not compare the proposed system with other existing electronic voting systems.

PAPER – 19

TITLE: Secure cloud e-voting system using fully homomorphic elliptical curve cryptography

AUTHOR: Anjima V.S., Hari N.N.

YEAR: 2019

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

This paper discusses the implementation of a secure cloud e-voting system based on Fully Homomorphic Elliptical Curve Cryptography (FHECC) scheme. Homomorphic encryption is an effective scheme for doing operations on encrypted data. It ensures that the votes hold its confidentiality by encrypting, and it allows adding votes without decryption. The paper compares FHECC with other homomorphic encryption algorithms like ElGamal and Paillier based on e-voting systems. The study shows that FHECC has better performance and improved security. The paper concludes that implementing a cloud e-voting system using FHECC increases security and confidentiality.

ADVANTAGES:

The implementation of a secure cloud e-voting system simplifies the traditional voting process from the point of view of both the voters as well as the officials. Voter turnout increases as the voting becomes easier and more convenient. The expense for human resources is drastically reduced as counting and tallying are all done by the software itself. FHECC ensures that privacy is preserved and the risk of the vote being tampered or leaked is minimum, even if the votes are stored in the public cloud. FHECC algorithm can effectively reduce the complexity of encryption and decryption. FHECC gives the same security as RSA with a key size of 164 bit.

LIMITATIONS:

The main problem while constructing a fully homomorphic encryption scheme is the homomorphic operations are time-consuming because the computations on large ciphertexts are typically slower than that in plaintext. The implementation of a secure cloud e-voting system using FHECC requires a certain level of technical expertise and resources, which may limit its accessibility to smaller organisations or governments.

PAPER – 20

TITLE: Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities.

AUTHOR: Harerimana R., Tan S.Y., Yau W.C.

YEAR: 2017

PUBLISHER: Institute of Electrical and Electronics Engineers Inc.

SUMMARY:

The paper discusses the implementation of an improved Paillier homomorphic encryption (HE) scheme in Java as an API. The authors analyse existing Paillier HE libraries and design a more efficient library. They also use their library to build an electronic voting system that allows for secure voting with voters remaining anonymous. The system records an average of only 2766ms for each vote placement through HTTP POST request.

ADVANTAGES:

The paper provides a solution for privacy violation by using homomorphic encryption, which allows mathematical operations on ciphertexts without knowledge of the plaintexts. The authors improve upon existing Paillier HE libraries and design a more efficient Java library. The electronic voting system built using their library provides a secure way for voters to vote while remaining anonymous.

LIMITATIONS:

The paper does not discuss the security of the implemented library or the electronic voting system in detail. The paper does not discuss potential limitations or drawbacks of using Paillier HE scheme in electronic voting or other applications. The paper does not provide a detailed comparison of their library's performance with other Paillier HE libraries or encryption schemes.

TOOLS USED:

Software: VS Code

Language: “C” Programming

OVERVIEW OF THE PROPOSED SYSTEM:

(Framework and Architecture for the Proposed System)

Paillier’s Algorithm:
This algorithm has a vast range of different applications like the banking security systems, in the area related to the cloud computing, etc.
Step 1: As it is an assymetric algorthim, a pair of keys are generated.

- Take two prime numbers a and b randomly which should be independent of each other such that $gcd(a*b,(a-1)*(b-1)) = 1$. GCD is the greatest common divisor of two or more integers which is the largest positive integer that divides the number without a remainder.
- Compute $n = (a*b)$ and also $k(n)=lcm((p-1),(q-1))$ where, k(n) is the Carmichael function.
- You should select a generator ‘g’ such that g belongs to the Zn.
- Calculate the follow Modular Multiplicative inverse:
  $u = (L(g^\wedge kmod\ n^\wedge 2))-1\ mod\ n$ where $L(u) = (u-1)/n$.

Public key: (n,g)
Private key: (k,u)

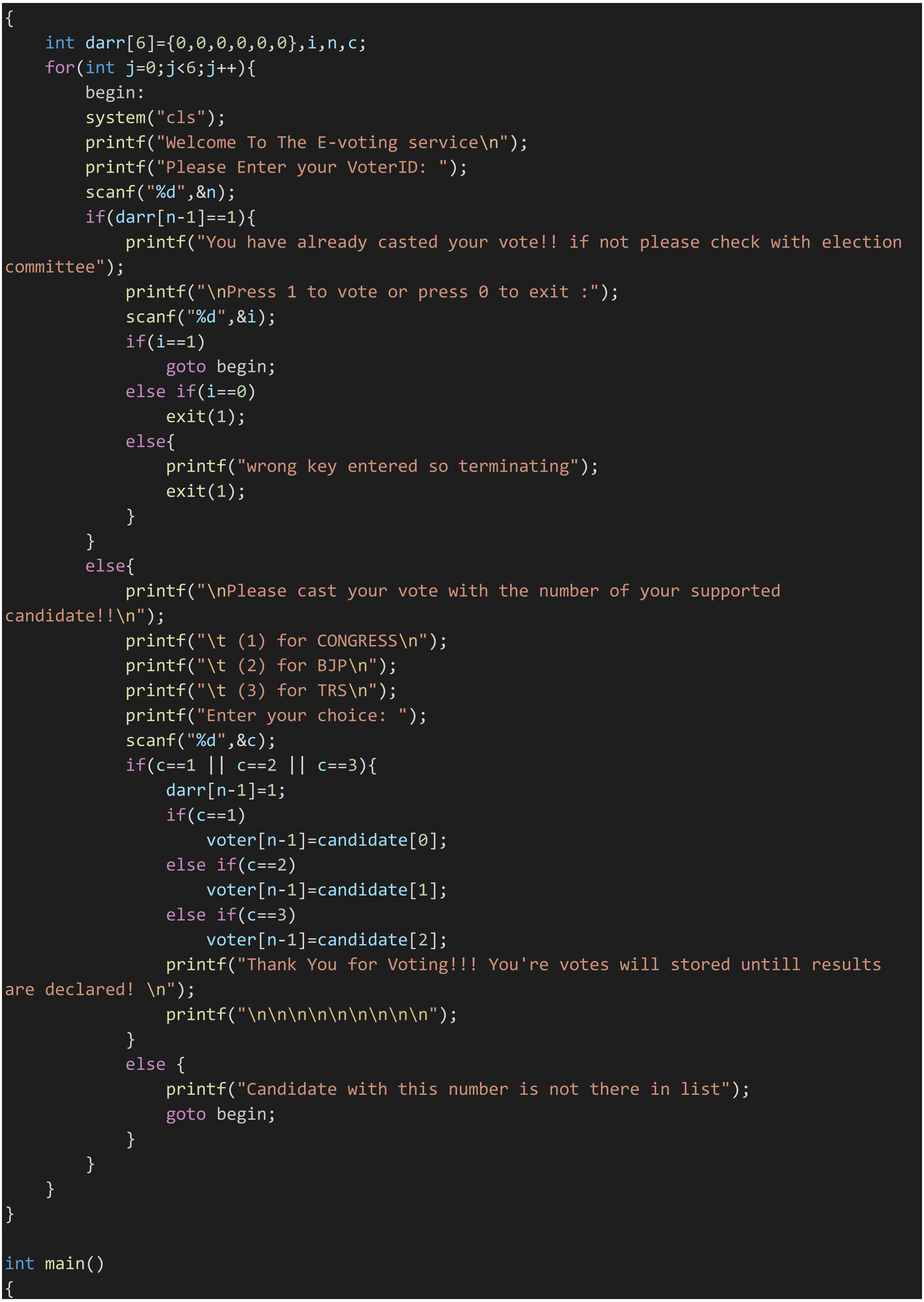
Step 2: Encryption process

- The message m needs to be encrypted where m belongs to the ‘z’.
- Now, choose a random number r.
- Compute cipher text $c = (gm * rn)mod\ n2$.

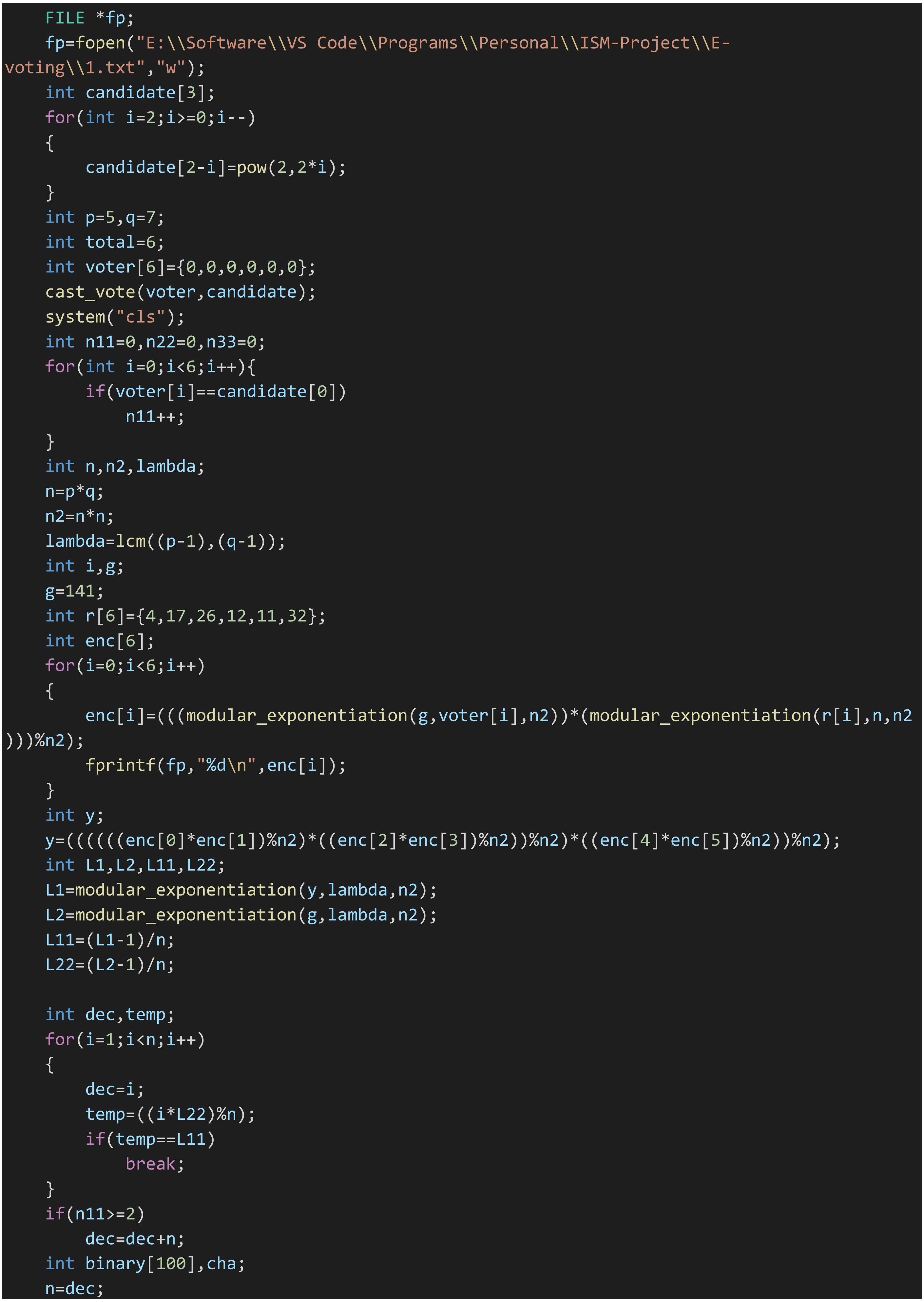
Step 3: Decryption process
Cipher text ‘c’ should be decrypted to get required message m as follows by using the private key(k,u) such that : $m = L(ck\ mod\ n2)* k\ mod\ n$.

IMPLEMENTATION CODE:

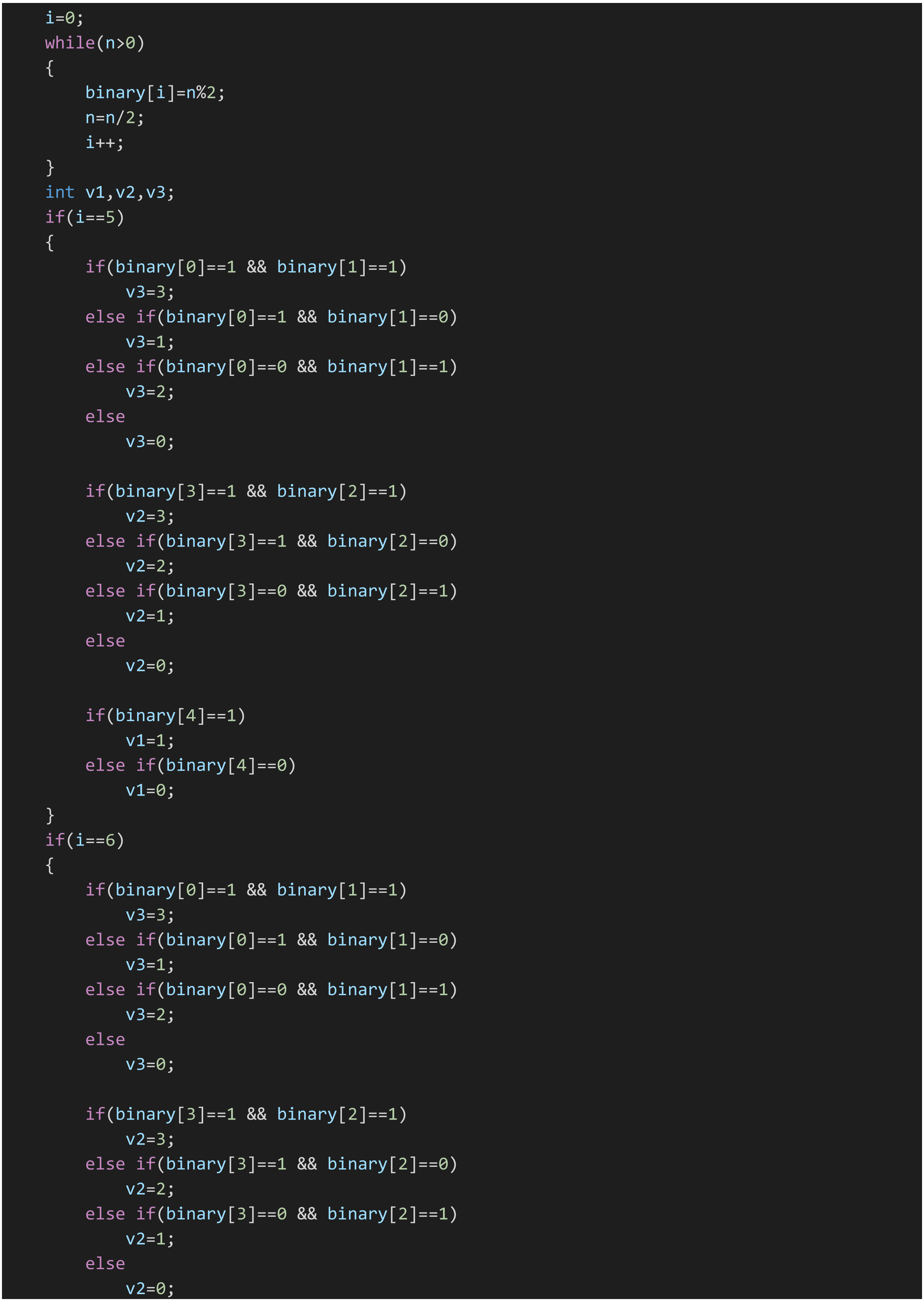
```
#include<stdio.h>
#include<stdlib.h>
#include<time.h>
#include<math.h>
#include<string.h>
#include<windows.h>

void decimal_to_binary(int d,int arr[]){
    int result,i=0;
    do{
        result=d%2;
        d/=2;
        arr[i]=result;
        i++;
    }while(d>0);
}

int lcm(int n1,int n2){
    int minMultiple;
    minMultiple = (n1>n2) ? n1 : n2;
    while(1)
    {
        if( minMultiple%n1==0 && minMultiple%n2==0 )
        {
            break;
        }
        ++minMultiple;
    }
    return minMultiple;
}

int modular_exponentiation(int a,int b,int n){
    int *bb;
    int count=0,c=0,d=1,i;
    count=(int)(log(b)/log(2))+1;
    bb=(int*)malloc(sizeof(int*)*count);
    decimal_to_binary(b,bb);
    for (i=count-1;i>=0;i--){
        c=2*c;
        d=(d*d)%n;
        if (bb[i]==1){
            c=c+1;
            d=(d*a)%n;
        }
    }
    return d;
}

void cast_vote(int* voter,int* candidate)
```



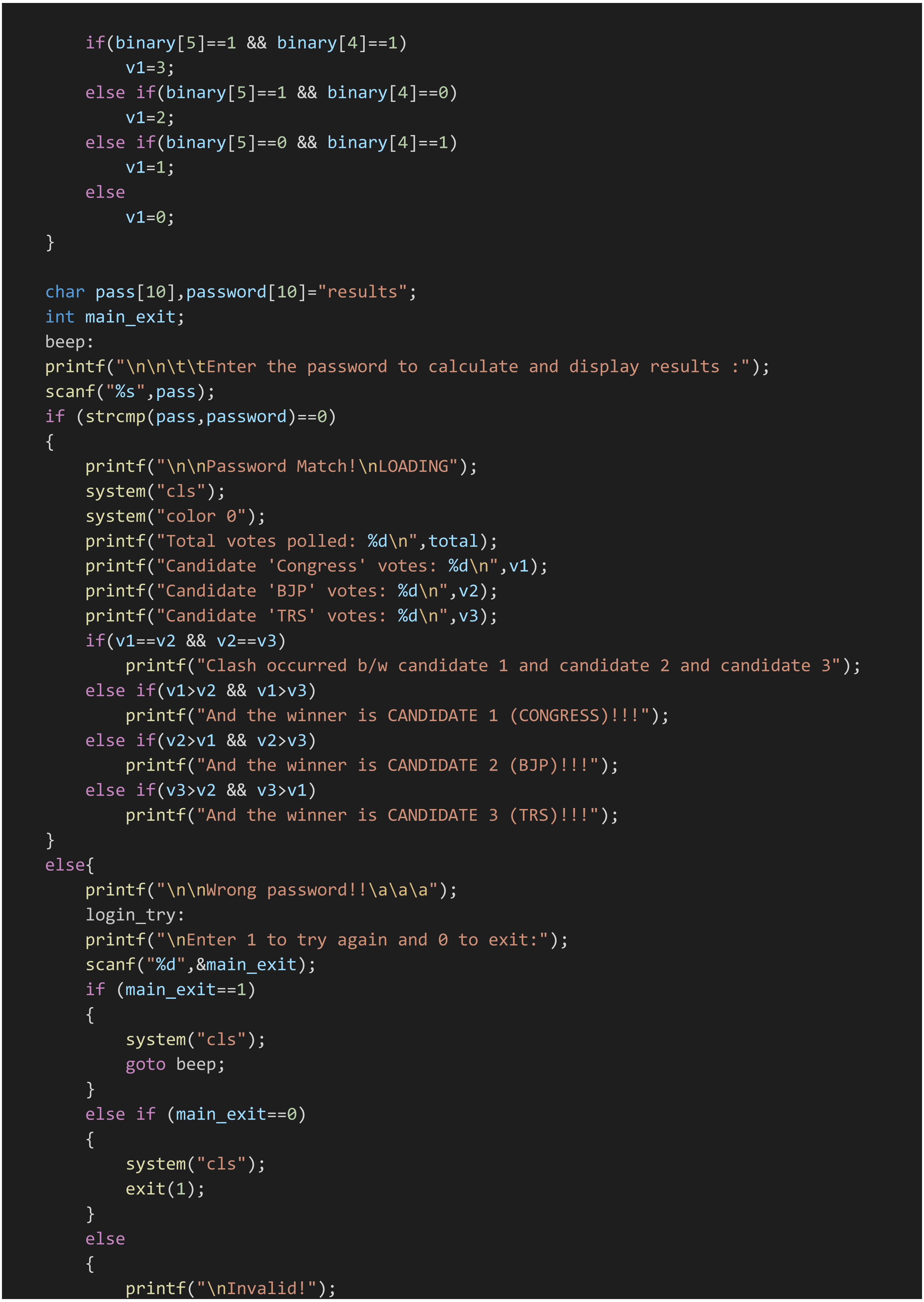
```
{
    int darr[6]={0,0,0,0,0,0},i,n,c;
    for(int j=0;j<6;j++){
        begin:
        system("cls");
        printf("Welcome To The E-voting service\n");
        printf("Please Enter your VoterID: ");
        scanf("%d",&n);
        if(darr[n-1]==1){
            printf("You have already casted your vote!! if not please check with election
committee");
            printf("\nPress 1 to vote or press 0 to exit :");
            scanf("%d",&i);
            if(i==1)
                goto begin;
            else if(i==0)
                exit(1);
            else{
                printf("wrong key entered so terminating");
                exit(1);
            }
        }
        else{
            printf("\nPlease cast your vote with the number of your supported
candidate!!\n");
            printf("\t (1) for CONGRESS\n");
            printf("\t (2) for BJP\n");
            printf("\t (3) for TRS\n");
            printf("Enter your choice: ");
            scanf("%d",&c);
            if(c==1 || c==2 || c==3){
                darr[n-1]=1;
                if(c==1)
                    voter[n-1]=candidate[0];
                else if(c==2)
                    voter[n-1]=candidate[1];
                else if(c==3)
                    voter[n-1]=candidate[2];
                printf("Thank You for Voting!!! You're votes will stored untill results
are declared! \n");
                printf("\n\n\n\n\n\n\n\n\n\n");
            }
            else {
                printf("Candidate with this number is not there in list");
                goto begin;
            }
        }
    }
}

int main()
{
```



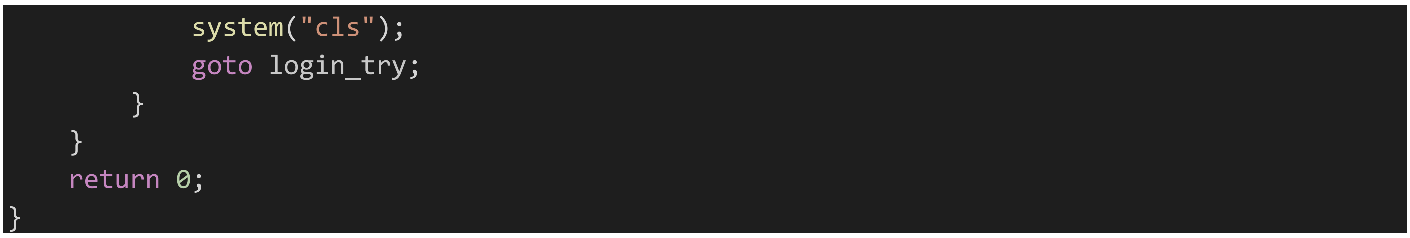
```
    FILE *fp;
    fp=fopen("E:\\Software\\VS Code\\Programs\\Personal\\ISM-Project\\E-
voting\\1.txt","w");
    int candidate[3];
    for(int i=2;i>=0;i--)
    {
        candidate[2-i]=pow(2,2*i);
    }
    int p=5,q=7;
    int total=6;
    int voter[6]={0,0,0,0,0,0};
    cast_vote(voter,candidate);
    system("cls");
    int n11=0,n22=0,n33=0;
    for(int i=0;i<6;i++){
        if(voter[i]==candidate[0])
            n11++;
    }
    int n,n2,lambda;
    n=p*q;
    n2=n*n;
    lambda=lcm((p-1),(q-1));
    int i,g;
    g=141;
    int r[6]={4,17,26,12,11,32};
    int enc[6];
    for(i=0;i<6;i++)
    {
        enc[i]=(((modular_exponentiation(g,voter[i],n2))*(modular_exponentiation(r[i],n,n2
)))%n2);
        fprintf(fp,"%d\n",enc[i]);
    }
    int y;
    y=((((((enc[0]*enc[1])%n2)*((enc[2]*enc[3])%n2))%n2)*((enc[4]*enc[5])%n2))%n2);
    int L1,L2,L11,L22;
    L1=modular_exponentiation(y,lambda,n2);
    L2=modular_exponentiation(g,lambda,n2);
    L11=(L1-1)/n;
    L22=(L2-1)/n;

    int dec,temp;
    for(i=1;i<n;i++)
    {
        dec=i;
        temp=((i*L22)%n);
        if(temp==L11)
            break;
    }
    if(n11>=2)
        dec=dec+n;
    int binary[100],cha;
    n=dec;
```



```
    i=0;
    while(n>0)
    {
        binary[i]=n%2;
        n=n/2;
        i++;
    }
    int v1,v2,v3;
    if(i==5)
    {
        if(binary[0]==1 && binary[1]==1)
            v3=3;
        else if(binary[0]==1 && binary[1]==0)
            v3=1;
        else if(binary[0]==0 && binary[1]==1)
            v3=2;
        else
            v3=0;

        if(binary[3]==1 && binary[2]==1)
            v2=3;
        else if(binary[3]==1 && binary[2]==0)
            v2=2;
        else if(binary[3]==0 && binary[2]==1)
            v2=1;
        else
            v2=0;

        if(binary[4]==1)
            v1=1;
        else if(binary[4]==0)
            v1=0;
    }
    if(i==6)
    {
        if(binary[0]==1 && binary[1]==1)
            v3=3;
        else if(binary[0]==1 && binary[1]==0)
            v3=1;
        else if(binary[0]==0 && binary[1]==1)
            v3=2;
        else
            v3=0;

        if(binary[3]==1 && binary[2]==1)
            v2=3;
        else if(binary[3]==1 && binary[2]==0)
            v2=2;
        else if(binary[3]==0 && binary[2]==1)
            v2=1;
        else
            v2=0;
```

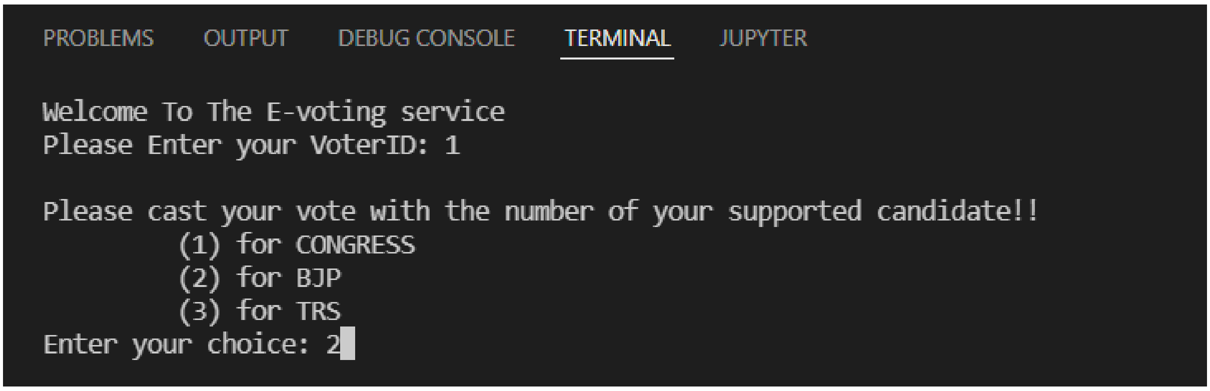


```
        if(binary[5]==1 && binary[4]==1)
            v1=3;
        else if(binary[5]==1 && binary[4]==0)
            v1=2;
        else if(binary[5]==0 && binary[4]==1)
            v1=1;
        else
            v1=0;
    }

    char pass[10],password[10]="results";
    int main_exit;
    beep:
    printf("\n\n\t\tEnter the password to calculate and display results :");
    scanf("%s",pass);
    if (strcmp(pass,password)==0)
    {
        printf("\n\nPassword Match!\nLOADING");
        system("cls");
        system("color 0");
        printf("Total votes polled: %d\n",total);
        printf("Candidate 'Congress' votes: %d\n",v1);
        printf("Candidate 'BJP' votes: %d\n",v2);
        printf("Candidate 'TRS' votes: %d\n",v3);
        if(v1==v2 && v2==v3)
            printf("Clash occurred b/w candidate 1 and candidate 2 and candidate 3");
        else if(v1>v2 && v1>v3)
            printf("And the winner is CANDIDATE 1 (CONGRESS)!!!");
        else if(v2>v1 && v2>v3)
            printf("And the winner is CANDIDATE 2 (BJP)!!!");
        else if(v3>v2 && v3>v1)
            printf("And the winner is CANDIDATE 3 (TRS)!!!");
    }
    else{
        printf("\n\nWrong password!!\a\a\a");
        login_try:
        printf("\nEnter 1 to try again and 0 to exit:");
        scanf("%d",&main_exit);
        if (main_exit==1)
        {
            system("cls");
            goto beep;
        }
        else if (main_exit==0)
        {
            system("cls");
            exit(1);
        }
        else
        {
            printf("\nInvalid!");
```

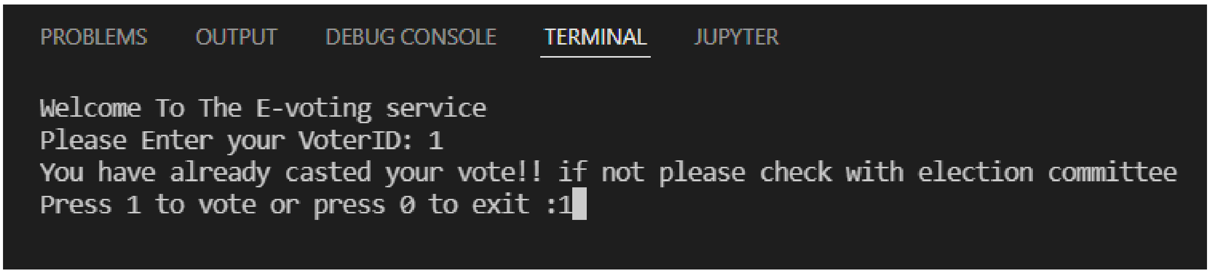


```
            system("cls");
            goto login_try;
        }
    }
    return 0;
}
```

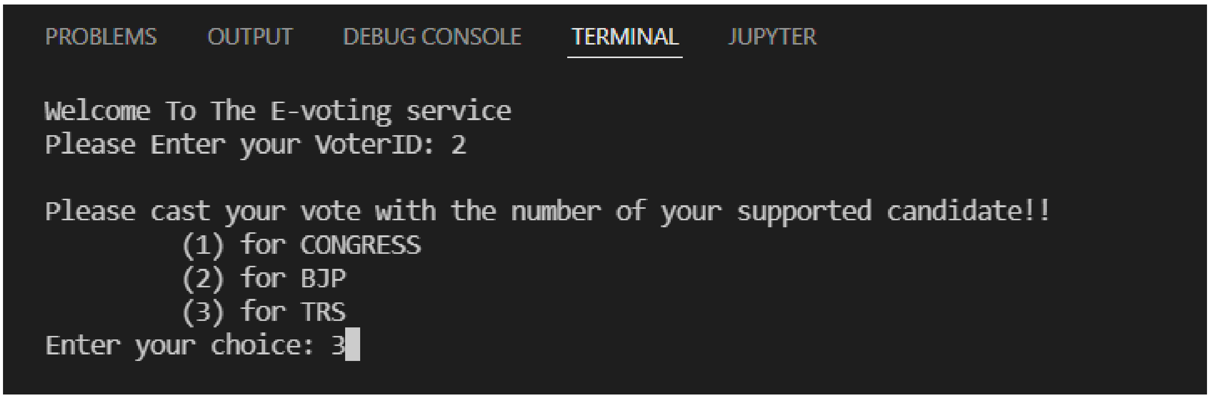
OUTPUT:



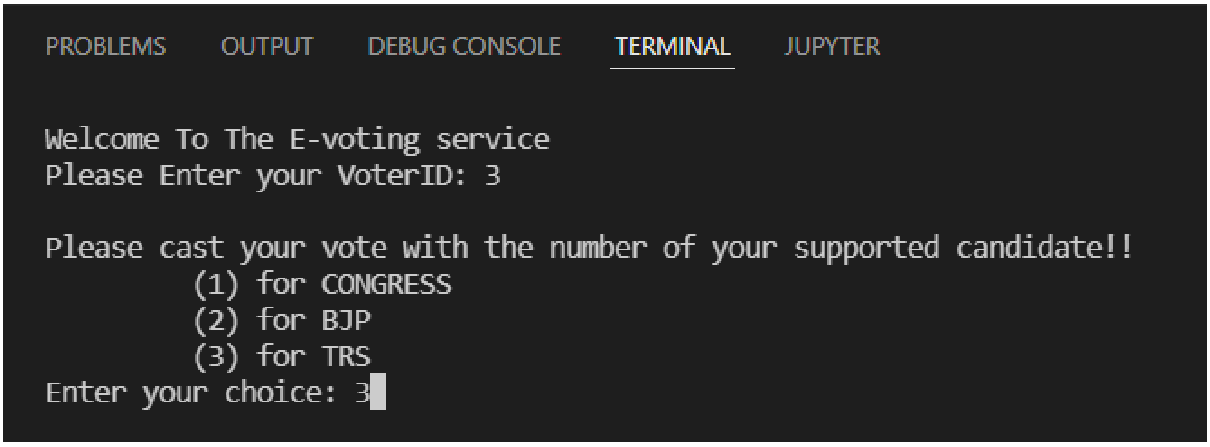
```
Welcome To The E-voting service
Please Enter your VoterID: 1

Please cast your vote with the number of your supported candidate!!
         (1) for CONGRESS
         (2) for BJP
         (3) for TRS
Enter your choice: 2
```



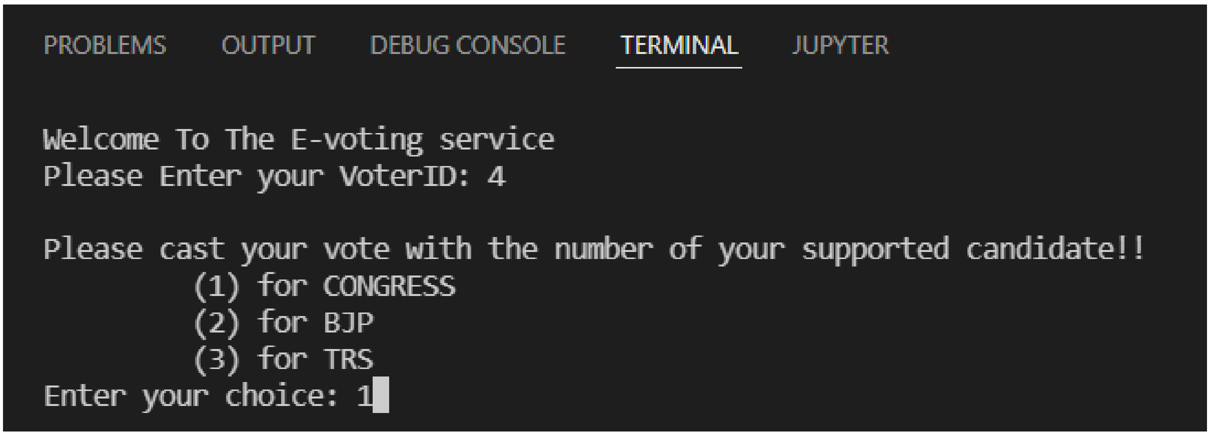
```
Welcome To The E-voting service
Please Enter your VoterID: 1
You have already casted your vote!! if not please check with election committee
Press 1 to vote or press 0 to exit :1
```



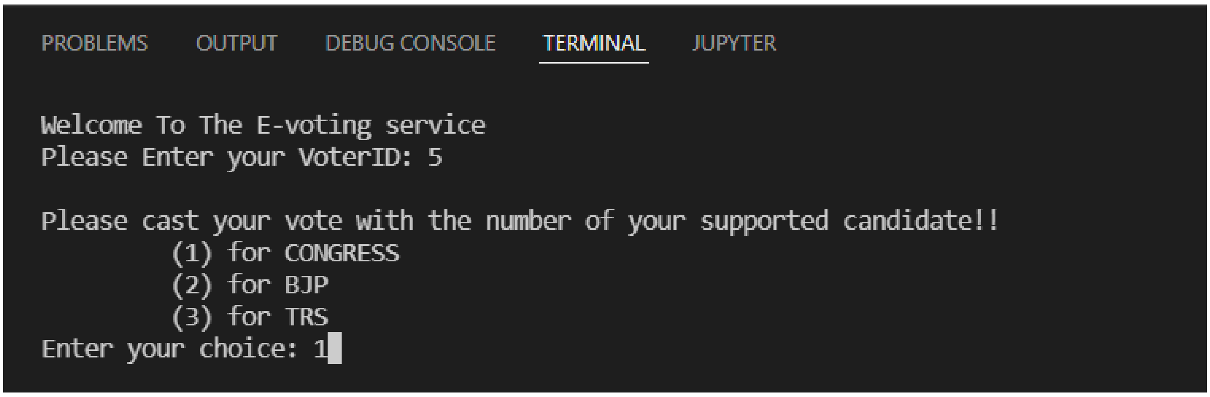
```
Welcome To The E-voting service
Please Enter your VoterID: 2

Please cast your vote with the number of your supported candidate!!
         (1) for CONGRESS
         (2) for BJP
         (3) for TRS
Enter your choice: 3
```



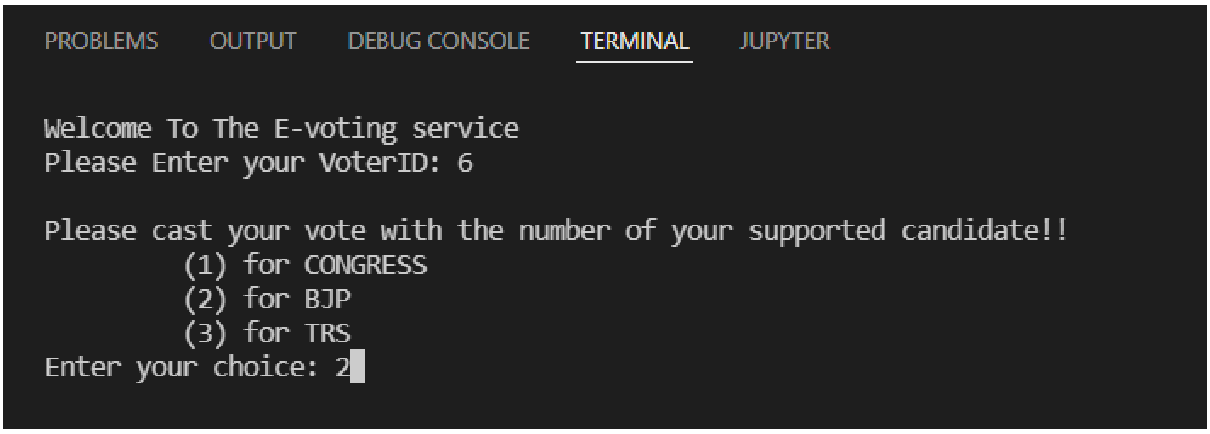
```
Welcome To The E-voting service
Please Enter your VoterID: 3

Please cast your vote with the number of your supported candidate!!
         (1) for CONGRESS
         (2) for BJP
         (3) for TRS
Enter your choice: 3
```



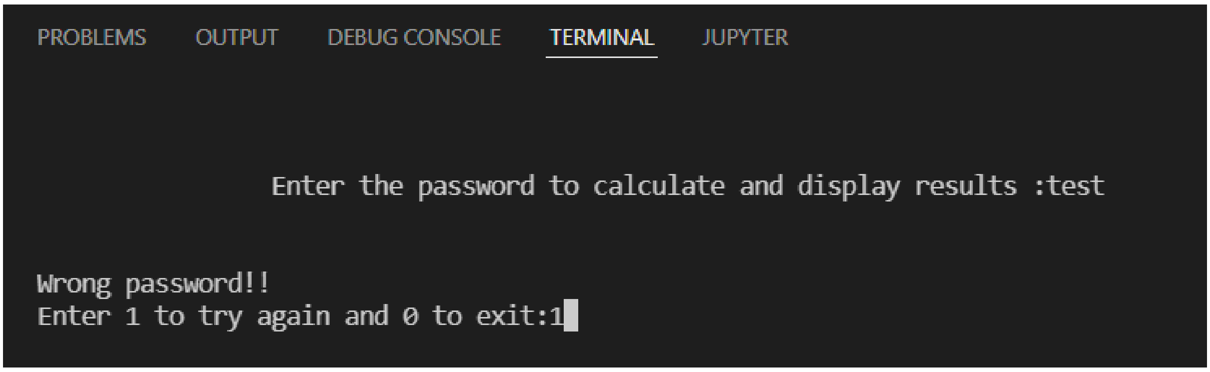
```
Welcome To The E-voting service
Please Enter your VoterID: 4

Please cast your vote with the number of your supported candidate!!
         (1) for CONGRESS
         (2) for BJP
         (3) for TRS
Enter your choice: 1
```



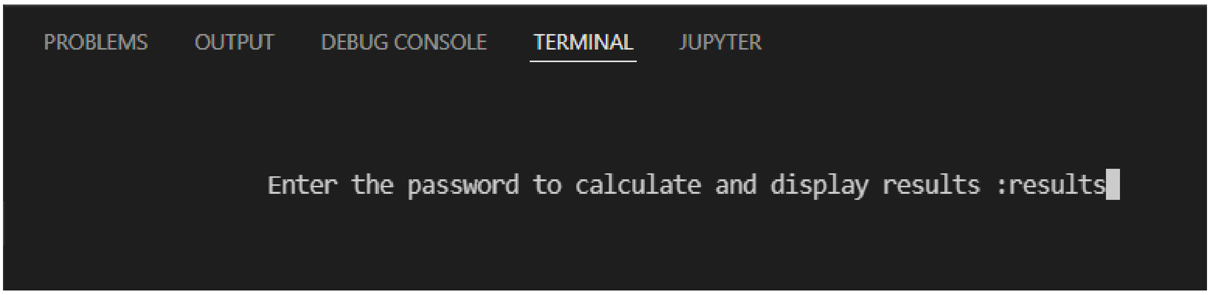
```
Welcome To The E-voting service
Please Enter your VoterID: 5

Please cast your vote with the number of your supported candidate!!
        (1) for CONGRESS
        (2) for BJP
        (3) for TRS
Enter your choice: 1
```



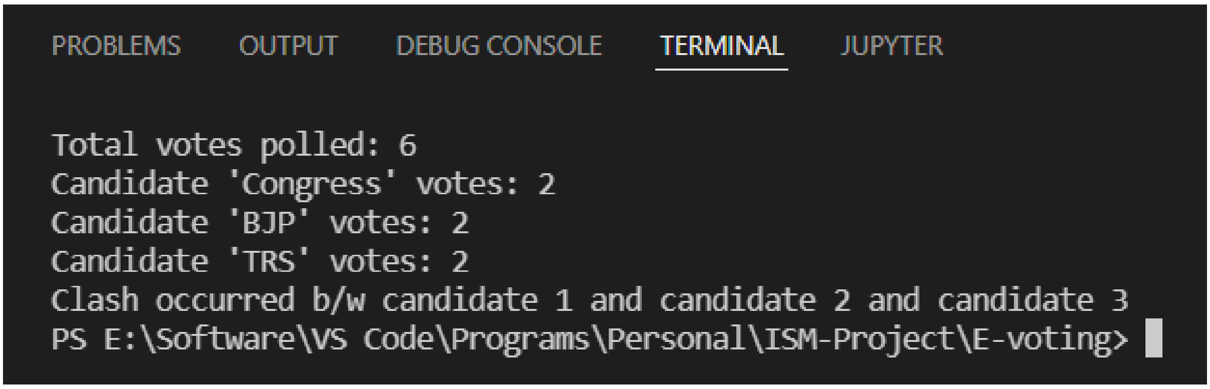
```
Welcome To The E-voting service
Please Enter your VoterID: 6

Please cast your vote with the number of your supported candidate!!
         (1) for CONGRESS
         (2) for BJP
         (3) for TRS
Enter your choice: 2
```



```
                Enter the password to calculate and display results :test


Wrong password!!
Enter 1 to try again and 0 to exit:1
```

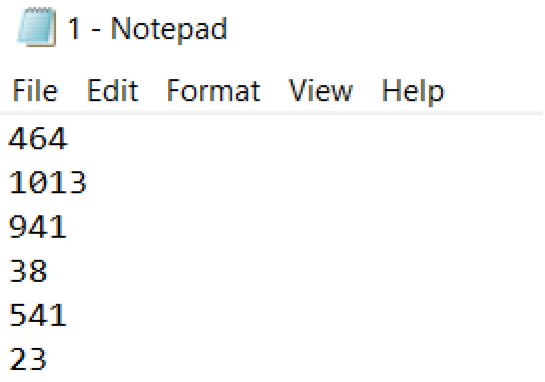


```
                Enter the password to calculate and display results :results
```



```
Total votes polled: 6
Candidate 'Congress' votes: 2
Candidate 'BJP' votes: 2
Candidate 'TRS' votes: 2
Clash occurred b/w candidate 1 and candidate 2 and candidate 3
PS E:\Software\VS Code\Programs\Personal\ISM-Project\E-voting>
```

Encrypted Votes:



```
464
1013
941
38
541
23
```

This file will be stored and sent for calculation and this is used to get the winner by decrypting the values

CONCLUSION:

In conclusion, the use of Paillier's homomorphic encryption algorithm in an e-voting system has been demonstrated to be a promising approach to ensuring secure and private elections. The system ensures the integrity and confidentiality of the voting process, allowing for efficient and convenient voting remotely from anywhere in the world. Additionally, the system is highly efficient and can be implemented at a lower cost than traditional voting methods, making it an attractive option for governments and organisations seeking to modernise their voting procedures. Given the potential to increase voter participation and engagement in the democratic process, the results of this project can be used as a foundation for future research and development of e-voting systems that prioritise security, privacy, and accessibility.